REMARKS

Claims 63-72 are pending in the present application.

Claims 69 and 72 stand rejected under 35 USC 112, first paragraph. Claim 71 stands rejected under 35 USC 102(b) as being anticipated by Toh et al. Claims 69, 70, and 72 stands rejected under 35 USC 103(a) as being obvious over Toh et al. Applicant has cancelled claims 69-72. Thus, these rejections are now moot.

Claim 63 stands rejected under 35 USC 112, first paragraph. The Examiner contends that the recitation of claim 63 which reads "(h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in said dated journal" is not described in the specification. Applicant respectfully disagrees with this analysis. Such operations are clearly based on the sequence of steps set out in FIGS. 1 and 2B of the original specification. The second data file of claim 63 corresponds to the "THIRD PARTY MDT" generated in block 32. The hash value for the second data file as recited in claim 63 corresponds to the "THIRD PARTY MDH" generated in block 33. The publication of the hash value for the second data file as recited in claim 63 corresponds to the publication of block 34. The comparison as recited in claim 63 corresponds to the compare operations following block 50 of FIG. 2A and described in the last paragraph of page 11 of the original specification. Moreover, original claim 28 of the present application explains that it is a hash value of

the second data file that is published for publication and comparison for authentication purposes.

For these reasons, the rejection of Claim 63 under 35 USC 112, first paragraph is clearly improper and should be removed.

Claim 67 stands rejected under 35 USC 112, first paragraph. The Examiner contends that the recitations of claim 67 directed to "the receiver transmitting the purported copy of said second hash value to the third party" is not described in the specification. Applicant respectfully disagrees with this analysis. Such receiver transmitting operations are clearly based on the fifth paragraph of page 4, second sentence, of the original specification, which reads "The recipient must now request the second Key from the third party by submitting the hash of the second message". It is also shown in step 410 of Fig 4C and described on page 28 of the original specification. For these reasons, the rejection of Claim 67 under 35 USC 112, first paragraph is clearly improper and should be removed.

Claims 63-66 stand rejected under 35 USC 103(a) as being unpatentable over Toh et al. in view of Haber et al. Claims 67-68 stand rejected under 35 USC 103(a) as being unpatentable over Toh et al. Applicant respectfully disagrees with the Examiner's analysis of the pending claims and requests reconsideration in light of the remarks herein.

The Examiner contends that the operations of (a) and (d) of claim 63 are disclosed by Toh and the operations of (b), (c), (e), (f), (g) and (h) are disclosed by Haber and that the combination of the disclosure of Toh with that of Haber would have been obvious and would have arrived at the invention as now claimed in claim 63. Such analysis is clearly improper as it is based on hindsight and furthermore misses a fundamental feature of the present invention.

To reiterate, Toh employs a hash algorithm on random data to generate a hash that is encrypted, together with a sender's private key, sent along with a data package from a sender to an operations center. The operations center uses the sender's public key to decrypt the hash value received from the sender, utilizes the same hash algorithm on the original random data to derive a hash value, and checks that the decrypted hash value matches the derived hash value in order to authenticate that the sender sent the message. Furthermore, as the examiner appears to acknowledge, Toh does not address the use of hash values to authentic a plurality of data items, let alone the steps of (b) to (h) as recited in claim 63.

Haber does not remedy the shortcomings of Toh. More specifically, Haber describes a user transmitting a request 20 to a remote service bureau. Although we accept that Haber discloses "publication" (at column 6), the relevant paragraph says that this is either causing the item itself to be directly published, or linking the item to another hash value that is directly published.

In contrast, the present invention of claim 63 involves transmission to a remote location of a single hash value derived from hash values for a plurality of stored data items, whereas Haber transmits to a remote location only a single hash value for particular document.

The transmission of a single hash value for a plurality of stored data items, which is a significant feature of the present invention, enables that plurality of documents all to be authenticated by the use of a single hash value, because that hash value is available in unviolatable and unimpeachable form in a dated journal of record published in numerous copies and held in separate public libraries. Whereas publication by a server such as that of Haber can be faked or otherwise compromised, it is inconceivable, that a dated journal of record published in numerous copies held in public libraries could be compromised in this way.

In other words, even if an entire audit trail has been compromised by an attacker, the resulting lack of integrity of the documents can be proved by reference to a publicly available source – namely one published in numerous copies in public libraries (for example, in the "Financial Times", which is the publication employed by the present assignee in their commercial operation of the present invention. All that someone (which can be the original party that generated the first data file and its hash value, or some other party) needs to do is to check the hash value in the published and dated journal, which then confirms whether the plurality of documents was hashed using the

hash value associated uniquely with one dated particular edition of the journal. The above is explained in detail on page 11 of the original specification.

Furthermore, a very significant advantage of the present invention is that authentication of a plurality of data items can be carried out in total anonymity, by comparison to the published hash value corresponding to the plurality of data items, where the publication is provided by an unimpeachable journal.

Thus, the cited prior art fails to teach or suggest important features of claim 63. For these reasons, claim 63 is clearly patentable over the cited prior art.

The dependent claims 64-68 are patentable over the cited prior art for those reasons advanced above with respect to claim 63 from which they respectively depend and for reciting additional features that are neither taught nor suggested by the cited prior art.

In light of all of the above, it is submitted that the claims are in order for allowance, and prompt allowance is earnestly requested. Should any issues remain outstanding, the Examiner is invited to call the undersigned attorney of record so that the case may proceed expeditiously to allowance.

Respectfully submitted,

/Jay P. Sbrollini/

Jay P. Sbrollini
Reg. No. 36,266
Attorney for Applicant(s)

GORDON & JACOBSON, P.C.
60 Long Ridge Road
Suite 407
Stamford, CT 06902
(203)323-1800

April 27, 2010